

Binary Subdivision for Quantum Search

M Nordin Zakaria
High Performance Computing Center,
Universiti Teknologi PETRONAS,
Perak, Malaysia
nordinzakaria@petronas.com.my

1 Introduction

More than a decade ago, Grover [5] discovered a quantum algorithm for searching unsorted list runs in $O(\sqrt{N})$. The algorithm is important as the best that can be attained classically with an unsorted list is in the order of $O(N)$. Since the publication of the work, there have been various improvements made to Grover's algorithm. Some work ([2],[4],[9],[10]) extends the result to other search-based algorithms, while others ([3],[7],[8],[13]) focusses on the nature of the unitary transformation involved in the search algorithm. The latter research direction is to be expected as in the words of Grover [6], the core of the algorithm is the "design of the unitary evolution of the system".

Though Grover's algorithm clearly outperforms its classical counterpart, it is still not 'fast' enough when applied to NP-complete problems. A straightforward application to the Travelling Salesman Problem, for example, following the approach in [4], results in an $O(\sqrt{n!})$ performance, where n is the number of cities. The result is still not computationally tractable for large values of n . This is surprising, as due to the inherent parallelism in quantum computation, one would expect a better result. Hence, in this paper, instead on focussing on the design of the unitary search evolution, we focus instead on the possibility of embedding a quantum search algorithm within a classical binary search framework. The result appears promising: taking full advantage of quantum parallelism, we show that it may actually be possible to search an unstructured list in $O(\lg(N))$, provided we are willing to restart the quantum search multiple times with a different sequence of qubits and perform a series of measurements at the end of each.

The gist of the idea in our research approach comes from a classical

algorithm within Computer Graphics and the Computational Geometry: ray tracing. In ray tracing, a ray is casted into a scene comprising of a number of objects. A brute force approach would test the ray against each and every object in the scene, a process that scales linearly with the number and the complexity of the objects. A smarter approach requires that the scene be partitioned into regions, and the bounding volume of each region be approximated. For each region, the ray would then be tested first against the bounding volume approximation. If the test is positive, then only would the ray be tested against each object within the region. Can a similar scheme be invented for Grover's algorithm? We would like to partition the list of items being searched into sublists. For each sublist, before we even perform repetitive amplification, we first check as to whether or not the desired item is somewhere within it. If the item is not there, we move on to the next sublist, and repeat the same query. We elaborate on this idea in the next section.

2 Binary Subdivision Algorithm

Our algorithm can be intuitively understood in classical terms as follows: We wish to search for an item, t , in an unsorted list, L . Suppose we are given a 'magic' function, F , that given L as input, instantaneously provide an output that indicates whether or not t is within the list. F does not pinpoint the location of t ; it merely says whether or not t is somewhere within the input list. We can then search using the following procedure:

Search(L)

1. *Divide L into two sublists: L_1 and L_2 .*
2. *Using F , check whether L_1 contains t . If yes, call $\text{Search}(L_1)$. If not, call $\text{Search}(L_2)$.*

Assuming that t exists in L , the recursive procedure will lead to t . We claim that F can be implemented as a quantum function, and that the overall procedure can be run classically.

As in Grover's algorithm, we start with 2 registers: n qubits in the first, and 1 qubit in the second. Note that the n qubits in the first register represents $N = 2^n$ numbers. In Grover's algorithm, the first register is initialized to be in the state $|Q\rangle = |0\rangle^{\otimes n}$, and the Hadamard operator, $H^{\otimes n}$, applied to it. The result is a linear combination of all 2^n computational basis states $|S\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$. The second register is initialized to $|1\rangle$,

and after a Hamadard transformation, comes to be in the state $|-\rangle$. Its sole purpose is to serve as the second qubit for the I_t oracle operator. Repeated application of Grover operator, $G = -HI_0HI_t$, is performed to increase the probability of obtaining the desired state, $|t\rangle$, when a measurement is made upon the first register. The I_t in the operator inverts the phase of $|t\rangle$. The I_0 operator inverts $|0\rangle$. Altogether, Grover operator works by amplifying the phase of the desired item, $|t\rangle$.

Instead of performing a quantum search on the entire list of items within $|S\rangle$, we wish to search only where $|t\rangle$ might be. Our approach requires two main features:

1. the ability to determine whether or not a state $|S\rangle$ contains $|t\rangle$. The function F described in the first paragraph of this section has this ability.
2. the ability to partition the list of items being searched into sublists.

The first feature is implemented by first running the oracle I_t in such a way that its second register is $|1\rangle$ for a target item, and $|0\rangle$ otherwise. Assuming that at most there can be only one target item, the resulting state of the second register will then be either $|0\rangle$ or $\sqrt{1 - 1/N}|0\rangle + 1/\sqrt{N}|1\rangle$. The distance between the 2 possible results decreases exponentially with increasing value of N . We show however how a series of non-unitary measurement operators with *non-negligible* probabilities of success can be used to differentiate between the two possible states.

As for the second feature, we note that the items in Grover's search do not actually exist as in a classical, conventional list. Instead the list is actually a single state, $|S\rangle$, that encodes a superposition of possible item values. We can however perform a partitioning by fixing qubits within $|Q\rangle$ and appropriately modifying the form of the Hamadard transform applied to it. As a specific example, consider the leftmost qubit, that is the one with the most significant digit. Half of the items in the state $|S\rangle$ that result after a $H^{\otimes n}$ operation on $|Q\rangle$ will start with $|0\rangle$ and the other half with $|1\rangle$. But if we fix the leftmost qubit in $|Q\rangle$ to be $|0\rangle$ (or $|1\rangle$) and perform a $I \otimes H^{\otimes n-1}$ instead, then the state $|S\rangle$ will only consists of items that start with $|0\rangle$ (or $|1\rangle$).

A more elaborate, formal elaboration of the proposed algorithm is then as follows: Let the initial state of the first register be $|Q\rangle = |q_0\rangle |q_1\rangle \dots |q_{n-1}\rangle$. Assume that we are now determining the value of the k^{th} qubit within the first register, where $0 \leq k < n$. Let b be a binary variable that contains the state value ($|0\rangle$ or $|1\rangle$) to be tried out for q_k . Let $|Q_0\rangle$ be the sublist of

$|Q\rangle$ for which the qubit values have already been determined. The general form of $|Q\rangle$ is then as follows: $(|Q_0\rangle |q_k\rangle |q_{k+1}\rangle \dots |q_{n-1}\rangle)$. Define as usual the function, $f : |0\rangle, \dots, |N-1\rangle \rightarrow 0, 1$, that recognizes the solution:

$$f(|i\rangle) = \begin{cases} 1 & \text{if } |i\rangle == |t\rangle \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Our algorithm then proceeds as follows:

1. Initialize $|Q_0\rangle$ to be a null list ($|\rangle$), and set $k = 0$, and $b = 0$. Initialize as well the second register to $|0\rangle$.
2. Repeat the following steps:
 - (a) Prepare the initial state $|Q\rangle = |Q_0\rangle |b\rangle |0\rangle |0\rangle \dots |0\rangle$.
 - (b) Perform $I^{\otimes k} \otimes H^{\otimes(n-k)}$ on $|Q\rangle$:

$$I^{\otimes k} \otimes H^{\otimes(n-k)}(|Q_0\rangle |b\rangle |0\rangle |0\rangle \dots |0\rangle) = |Q_0\rangle |b\rangle \frac{\sum_{i=0}^{2^{n-k-1}} |i\rangle}{\sqrt{2^{n-k-1}}} = |\psi\rangle \quad (2)$$

- (c) Perform I_t on $|\psi\rangle |0\rangle$:

$$I_t |\psi\rangle |0\rangle = I_t \left(|Q_0\rangle |b\rangle \frac{\sum_{i=0}^{2^{n-k-1}} |i\rangle}{\sqrt{2^{n-k-1}}} |0\rangle \right) \quad (3)$$

$$= |Q_0\rangle |b\rangle \frac{\sum_{i=0}^{2^{n-k-1}} |i\rangle |0 \oplus f(|Q_0\rangle |b\rangle |i\rangle)\rangle}{\sqrt{2^{n-k-1}}} \quad (4)$$

- (d) Consider the 2 possible results when the second register is measured:

- If the target item is not within $|\psi\rangle$, then the result of the observation will be $|y\rangle = |0\rangle$. Otherwise, it will be

$$|x\rangle = \sqrt{1 - \frac{1}{N}} |0\rangle + \frac{1}{\sqrt{N}} |1\rangle \quad (5)$$

where $N = 2^n$. Assume for now that it is possible to differentiate between $|x\rangle$ and $|y\rangle$. Hence, we can proceed as follows:

- Suppose the target item is not within $|\psi\rangle$. Then if $b == 0$, we set $b = 1$ and repeat step 2.

- If the target item is within $|\psi\rangle$, we then append $|q_k\rangle$ to $|Q_0\rangle$ - its state value considered fixed -, and proceed on by repeating step 2 with $b = 0$ and $k = k + 1$.

The complexity of the above algorithm, in terms of the number of queries to the oracle, assuming that we perform recursive subdivision without actually doing any amplitude amplification, is obviously $lg(2^n)$.

3 Differentiating between $|x\rangle$ and $|y\rangle$

We need to differentiate between

$$|x\rangle = \sqrt{\frac{N-1}{N}} |0\rangle + \frac{1}{\sqrt{N}} |1\rangle \quad (6)$$

and

$$|y\rangle = |0\rangle \quad (7)$$

The dot product between the two however approaches 1 with increasing N , that is $\sqrt{(N-1)/N} \rightarrow 1$ when $N \rightarrow \infty$. Nevertheless, if it is possible to apply a transformation using the following matrix, we would be able to tell the two apart:

$$D = \begin{pmatrix} 1 & -\sqrt{N-1} \\ 0 & \sqrt{N} \end{pmatrix} \quad (8)$$

Note that:

$$D |x\rangle = |1\rangle \quad (9)$$

and

$$D |y\rangle = |0\rangle \quad (10)$$

Unfortunately, D is not a unitary matrix. It is however possible to apply a non-unitary operator as a quantum measurement operator, as proposed in the work by Terashima and Ueda [12]. We need to convert D into an operator that is implementable as a quantum operator. To do this we perform the following transformation steps:

1. We first factor D using Singular Value Decomposition (SVD):

$$D = QVR^T \quad (11)$$

Q and R are unitary matrices, while V is a diagonal matrix. Q and R can be implemented easily within a unitary quantum framework. We

are left with V , a 2×2 diagonal matrix that comes with one very large and one very small diagonal value. For example, if $n = 10$, V would be:

$$V = \begin{pmatrix} 45.249308037472204 & 0 \\ 0 & 0.707193134832027 \end{pmatrix} \quad (12)$$

And if $n = 30$, V would be:

$$V = \begin{pmatrix} 46340.95000644678 & 0 \\ 0 & 0.70710678127 \end{pmatrix} \quad (13)$$

2. We now factor V into its roots, such that the first diagonal element becomes a value less than 2. The power of the root depends on the size of the first diagonal element. If we take the 16^{th} root of V , for example, we obtain

$$V = V_{1/16} V_{1/16} \dots V_{1/16} \quad (14)$$

where $V_{1/16}$ is applied 16 times.

In the case of $n = 30$, $V_{1/16}$ would be as follows:

$$V_{1/16} = \begin{pmatrix} 1.957144124161160 & 0 \\ 0 & 0.978572062094820 \end{pmatrix} \quad (15)$$

3. We then normalize the diagonal elements of $V_{1/16}$. Let M_0 be the resulting matrix. In the case of $n = 30$, $V_{1/16}$ matrix would then become

$$M_0 = \begin{pmatrix} 0.894427190997313 & 0 \\ 0 & 0.447213595505164 \end{pmatrix} \quad (16)$$

The sequence of transformation to be applied to either $|x\rangle$ or $|y\rangle$ is then in the following order:

1. R^\dagger
2. $M_0 \dots M_0$ (v times where v indicates the power of the root of V applied to obtain $V_{1/v}$)
3. Q

We prepare the matrices used in the above sequence for each of the possible values of n encountered in the quantum binary search in Section 2.

Note that the measurement operator complementary to M_0 is computed as follows [12]:

$$M_1 = \sqrt{1 - M_0^\dagger M_0} \quad (17)$$

The effect of M_0 on a state $|\psi\rangle$ is computed as follows:

$$|\psi\rangle \rightarrow \frac{M_0 |\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} \quad (18)$$

3.1 Example

We consider as a complete numerical example, the case when $n = 20$. Suppose the target item is within the state in the first register. The state of the second register will then be:

$$x = 0.999999523162728 |0\rangle + 0.000976562500000 |1\rangle \quad (19)$$

The matrix D that we want is:

$$D = \begin{pmatrix} 1 & -1023.999511718634 \\ 0 & 1024.0 \end{pmatrix} \quad (20)$$

Performing SVD, we obtain $D = QVR^T$ where

$$Q = \begin{pmatrix} -0.707106781186547 & -0.707106781186547 \\ 0.707106781186547 & -0.707106781186547 \end{pmatrix} \quad (21)$$

$$V = \begin{pmatrix} 1448.154515236507 & 0 \\ 0 & 0.707106865480 \end{pmatrix} \quad (22)$$

and

$$R = \begin{pmatrix} -0.000488281308208 & -0.999999880790675 \\ 0.999999880790675 & -0.000488281308208 \end{pmatrix} \quad (23)$$

Now,

$$V^{1/16} = \begin{pmatrix} 1.575980833365910 & 0 \\ 0 & 0.978572069378633 \end{pmatrix} \quad (24)$$

Normalizing the matrix (along the diagonal), we obtain M_0 , a non-unitary measurement operator:

$$M_0 = \begin{pmatrix} 0.849549077650853 & 0 \\ 0 & 0.527509587270776 \end{pmatrix} \quad (25)$$

With the matrices above prepared (in an offline process), we follow the proposed sequence of steps. We start off by applying the unitary operator R to obtain:

$$|d\rangle = 0.000488281308208 |0\rangle - 0.999999880790675 |1\rangle \quad (26)$$

We go now into the non-unitary phase, where M_0 is to be applied 16 times. Consider the effect of just the first iteration. Note that the success probability in applying M_0 is 0.278266470393446. After applying M_0 , state becomes:

$$|d\rangle = 0.000786372165026 |0\rangle - 0.999999690809361 |1\rangle \quad (27)$$

We assume for now (in this paper) that M_0 is successful throughout the non-unitary phase. Note that the success probability in applying M_0 in this particular example is in the range from about 0.28 to about 0.40.

At the end of the 16 applications of M_0 , the state becomes:

$$|d\rangle = 0.707106781186547 |0\rangle - 0.707106781186548 |1\rangle \quad (28)$$

Applying Q , the state finally becomes:

$$|d\rangle = 0 |0\rangle + 1 |1\rangle \quad (29)$$

4 Notes

We make a few notes with regard to the method proposed in this paper.

1. Quantum search using binary trees has been considered in other works, for example [9]. However, the binary tree search proposed in this paper does not assume sorted data.
2. An alternative approach for differentiating between $|x\rangle$ and $|y\rangle$ is described by Ohya and Volovich in [11]. They propose the use of what they call a *chaotic amplifier* to separate the two states. The method proposed in this paper, however, should be easier to understand and implement.
3. While it has been proven before that a black-box quantum query algorithm cannot solve NP problems in $o(2^{n/2})$ [1], the approach in this paper incorporates non-unitary model, and hence it does not violate the result in [1].

4. The main catch in the proposed method is that in the state differentiation module, we have not considered the case when M_1 instead of M_0 was applied during the non-unitary phase, resulting in the intermediate result $|d'\rangle$ rather than $|d\rangle$. In some cases, $|d'\rangle$ is far enough from $|d\rangle$ so as to be easily distinguishable. In general, some sort of statistical scheme would be needed to ensure that the final result used is one obtained without or with minimal application of M_1 .

References

- [1] C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. arXiv:quant-ph/9701001.
- [2] G. Brassard, P. Høyer, and A. Tapp. Quantum counting. In *Proceedings of 25th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science*, volume 1443, pages 820–831. Springer-Verlag, July 1998.
- [3] N.J. Cerf, L.K. Grover, and C.P. Williams. Nested quantum search and np-complete problems, June 1998. arXiv:quant-ph/9806078v1.
- [4] C. Durr and P. Høyer. A quantum algorithm for finding the minimum, July 1996. arXiv:quant-ph/9607014v2.
- [5] L. Grover. A fast quantum mechanical algorithm for database searching. In *ACM Symposium on Theory of Computing*, pages 212–219. ACM, 1996.
- [6] L. Grover. Quantum computers can search rapidly by using almost any transformation. In *Physical Review Letters*, volume 80, pages 4329–4332, May 1998.
- [7] L. Grover. A different kind of quantum search, March 2005. arXiv:quant-ph/0503205v1.
- [8] L. K. Grover. Superlinear amplitude amplification, June 2008. arXiv:0806.0154v1.
- [9] P. Høyer, J. Neerbek, and Y. Shi. Quantum complexities of ordered searching, sorting and element distinctness, April 2001. arXiv:quant-ph/0102078v2.

- [10] A. Nayak and F. Wu. The quantum query complexity of approximating the median and related statistics, November 1998. arXiv:quant-ph/9804066v2.
- [11] M. Ohya and I.V. Volovich. A new quantum algorithm for np-complete problems, September 2002. CDMTCS Research Report Series.
- [12] H. Terashima and M. Ueda. Nonunitary quantum circuit, April 2005. arXiv:quant-ph/0304061v5.
- [13] R.R. Tucci. An adaptive, fixed-point version of grover's algorithm, September 2010. arXiv:1001.5200v2.